



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/621,056	07/21/2000	David W. Carman	NTWK005/05US	4462

28875 7590 06/07/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP  
P.O. BOX 721120  
SAN JOSE, CA 95172-1120

EXAMINER

HO, THOMAS M

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 06/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

21

## Office Action Summary

Application No.

09/621,056

Applicant(s)

CARMAN ET AL.

Examiner

Thomas M Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 18 March 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-5 and 7-26 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) 5 and 7-26 is/are allowed.
- 6) ☒ Claim(s) 1-4 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

1. **Claims 1-5, 7-26 are pending.**
2. The terminal disclaimer filed on 3/18/04 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of 09/621056, 09/621057, 09/621058, 09/621059, and 09/621060 has been reviewed and is accepted. The terminal disclaimer has been recorded.
3. Claims 5, 7-26 allowed.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Bellare et al.

In reference to claim 1:

Art Unit: 2134

Bellare et al. (HMAC: A practical variant, pages 13-15) discloses a method for generating an authentication tag for a message that can be used for error correction comprising:

- Processing a portion of the message using a reversible first function to produce an intermediate result, where the intermediate result is inner hash function that must be produced.  $(\text{HMAC}(x) = F(k, \text{pad1}, F(k, \text{pad2}, x))$
- Processing the intermediate result with a second function to produce the authentication tag, where the intermediate result is then set as one of the arguments for the HMAC function.
- Encrypting the intermediate result, where the intermediate result is enciphered or “encrypted” by the virtue of the hash function.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 3,4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellare et al.

In reference to claim 3:

Bellare et al. fails to explicitly disclose a method further comprising sending the intermediate result to a receiver of the message.

Art Unit: 2134

The Examiner takes official notice that sending intermediate results of computations to another computer to complete the computation was well known in the art at the time of invention.

In fact, dividing a complex computation too to share the load with other computer is one of foundations of distributed computing. This is also a prevalent model in computing with client/server models where oftentimes, a greater burden of a given computation will be set on the client so that the server can better tend to other client requests.

Bellare et al. (1.1 Authenticity and MACs, pages 2) further teaches that in order for a MAC to be verified, the receiver must also compute the value of the authentication tag.

It would have been obvious to one of ordinary skill in the art at the time of invention to send the intermediate result of the authentication tag computation to the receiver of the message given that the receiver needs to compute the full authentication tag in any case, and to lighten the computational burden on the receiver or to provide another value with which the receiver can compare to authenticate the sender.

In reference to claim 4:

Bellare et al. (1.1 Authenticity and MACs, pages 2) discloses a method further comprising sending the authentication tag to the receiver of the message.

*Conclusion*

7. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

Application/Control Number: 09/621,056

Page 6

Art Unit: 2134

May 27<sup>th</sup> 2004

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100